Dependable Computer Networks

D. Avresky

Network Computing Lab., ECE Department
Northeastern University
Dana Research Bldg.
Boston, MA 02115
avresky@ece.neu.edu

January 2, 2002

Within several years, it will be common to have private networked computing systems, which will encompass tens of thousands of computing devices. Some of these networks (military, banking, e-business, transportations) will run mission-critical applications. The challenge is to build computer networks, based on COTS, that are inexpensive, accessible, scalable and dependable. Private virtual networks are created by composing a complex set of hardware and software components that are heterogeneous and subject to continuous upgrade, replacement, and scaling their numbers. These systems are too complex to model formally, and reducing the failure rate of individual components may not substantially reduce the rate of overall system failures due to unexpected interactions between components. One may consider that failures are inevitable. Having this in mind, we have to consider detection and recovery-oriented computing, a technique for achieving high availability that focuses on detecting and recovering from failures rather than preventing them entirely.

Dependability of service is of paramount concern for industrial and military applications when information is required. In addition to being continuously available, these systems must be free from data corruption. Absolute data integrity must be ensured through full self-checking and fault isolation. As the number of components increases, so does the probability of component failure. Therefore, a fault-tolerant technology is required in networked environments. Thus, one of the objectives of the research is to increase the dependability of scalable networked systems.